IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO. 1:15-CR-309**
	:	
v.	:	**(Chief Judge Conner)**
	:	
JALIL IBN AMEER AZIZ	:	
	:	
Defendant	:	

MEMORANDUM

Defendant Jalil Ibn Ameer Aziz ("Aziz") moves the court for notice and disclosure of surveillance under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, and to suppress the fruits of such surveillance or any other collection conducted pursuant to FISA, or other "confidential" foreign intelligence gathering, or any parallel construction or "scrubbing" activities. (Doc. 62). For the reasons articulated herein, the court will deny Aziz's motion.

I. Factual Background and Procedural History

The United States commenced prosecution of Aziz on December 17, 2015, with the filing of a criminal complaint. (Doc. 3). On December 22, 2015, a federal grand jury sitting in Harrisburg, Pennsylvania, returned a two-count indictment charging Aziz with conspiracy (Count I) and attempt (Count II) to provide material support and resources to a designated foreign terrorist organization, to wit: the Islamic State of Iraq and the Levant ("ISIL"), in violation of 18 U.S.C. § 2339B(a)(1). (Doc. 13). The government thereafter filed its first notice (Doc. 21) pursuant to 50 U.S.C. § 1825(d) of intent to use FISA information obtained or derived from physical searches.

On April 13, 2016, the court scheduled a pretrial conference pursuant to Section 2 of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. III § 2. (Doc. 32). The court agreed with the parties that the complexity of these proceedings, in particular the anticipated CIPA and FISA motion practice, warranted a continuance of the trial date to February 6, 2017. (Doc. 38). The court also reviewed and approved the parties' proposed schedule for pretrial motion practice. (Doc. 39). In pertinent part, the court set September 6, 2016, as Aziz's deadline to submit any FISA suppression motion. (Id.)

On May 18, 2016, the grand jury returned a superseding indictment reiterating Counts I and II and further charging Aziz with solicitation to commit a crime of violence in violation of 18 U.S.C. §§ 2 and 373 (Count III) and transmitting a communication containing a threat to injure in violation of 18 U.S.C. §§ 2 and 875(c) (Count IV).[1] (Doc. 42). The superseding indictment specifically avers in support of Count IV that Aziz, via Twitter, transmitted a communication providing "names, addresses, photographs, and branches of the military of approximately one hundred United States servicemen" which communication urged: "[K]ill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking that they are safe." (Doc. 42 at 3-4). On August 4, 2016, the government filed a second notice (Doc. 56) of intent to use FISA information, this time identifying an intent to use evidence obtained or derived from both physical searches and electronic surveillance. Aziz's instant motion followed.

[1] The superseding indictment included 18 U.S.C. § 2 as an additional substantive basis for Count II. (See Doc. 42 at 2).

II. The Foreign Intelligence Surveillance Act

Congress enacted FISA in response to perceived abuses of intelligence-gathering and surveillance procedures by federal intelligence agencies in the early 1970s. See Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 792-93 (2d Cir. 2015). The act establishes a statutory framework under which executive branch agencies may conduct surveillance and searches in foreign intelligence investigations. See 50 U.S.C. § 1801 *et seq.* FISA authorizes the Chief Justice of the United States to designate eleven district court judges to sit as judges on the Foreign Intelligence Surveillance Court ("FISC"). Id. § 1803(a)(1). FISC judges review and resolve the government's *ex parte* applications for orders permitting surveillance or searches. See id. FISA also establishes the Foreign Intelligence Court of Review ("FICR"), comprised of three district court or circuit court judges, to review decisions of the FISC. Id. § 1803(b).

The statute as originally enacted required a high-ranking member of the executive branch "to certify that 'the purpose' of the surveillance is to obtain foreign intelligence information." United States v. Duka, 671 F.3d 329, 338 (3d Cir. 2011) (emphasis added) (quoting *In re* Sealed Case, 301 F.3d 717, 723 (FISA Ct. Rev. 2002)). In 2001, Congress enacted the Patriot Act.[2] Among other things, the Patriot Act amended FISA to require certification that foreign intelligence gathering is "a significant purpose" rather than "the purpose" of the surveillance or search intended. Duka, 671 F.3d at 336-37 (3d Cir. 2011). Prior to passage of the Patriot

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

Act, courts construed "the purpose" to mean "the primary purpose" of the proposed surveillance or search. Id. (citing United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984)); *In re* Sealed Case, 310 F.3d at 725-26 (collecting cases). Courts have held that the 2001 Patriot Act amendments evinced Congress's intent to relax the juridical "primary purpose" standard. *In re* Sealed Case, 310 F.3d at 733; United States v. Hasbajrami, No. 11-CR-623, 2016 WL 1029500, at *4 (E.D.N.Y. Feb. 18, 2016) (citing United States v. Abu-Jihaad, 630 F.3d 102, 119 (2d Cir. 2010)); United States v. Kashmiri, No. 09-CR-830, 2010 WL 4705159, at *4 (N.D. Ill. Nov. 10, 2010).

FISA's application requirements are rigorous by design. The statute obliges the government to make detailed factual showings about the target of the proposed surveillance or search, the information sought, and the facilities at which the surveillance or search are directed. See 50 U.S.C. §§ 1804(a), 1823(a). The application must be personally reviewed and approved by the Attorney General of the United States before submission to the FISC. Id. §§ 1804(d), 1823(d).

FISA authorizes the government to use information obtained or derived from FISC-authorized electronic surveillance or physical searches in federal, state, or local criminal prosecutions. Id. §§ 1806(a), 1825(a). The government must provide notice to the court and to each "aggrieved person" of its intent to disclose or to use such information. Id. §§ 1806(c), 1825(d). The "aggrieved person" may then move to suppress FISA-acquired evidence on grounds that "the information was unlawfully acquired" or the surveillance or search "was not made in conformity with an order of authorization or approval." Id. §§ 1806(e), 1825(f).

III. Discussion

Aziz filed the instant motion to suppress and for disclosure of FISA-related information pursuant to 50 U.S.C. §§ 1806(e) and 1825(f). (Doc. 62). Aziz moors his requests in a combination of procedural, statutory, and constitutional challenges to FISA generally and as applied in this case. (See Doc. 63). Aziz asserts: (1) that he is entitled to discovery of the government's FISA applications and any supporting materials, and that failure to disclose this material violates his rights under the United States Constitution; (2) that the underlying FISA applications may contain intentional or reckless material falsehoods or omissions in violation of Franks v. Delaware, 438 U.S. 154 (1978); and (3) that the government may not have fully complied with the statute in its application for or implementation of the FISA orders. (See Doc. 63 at 10-12).[3] The court will address these issues *seriatim*.

A. Notice and Disclosure

FISA's statutory language is unequivocal that disclosure of warrant applications and supporting materials is the exception, not the rule. See 50 U.S.C. §§ 1806(f), 1825(g). When, in answer to a suppression motion, the Attorney General files an affidavit stating "under oath that disclosure or an adversary hearing would harm the national security," the district court "shall . . . review *in camera* and *ex parte* the application, order, and such other materials relating to" the surveillance

[3] Aziz speculates that the government may have violated other provisions of FISA or the First and Fourth Amendments in manners yet unknown to him. (Doc. 63 at 12). Given the veiled nature of FISA proceedings, we do not fault counsel for arguments grounded in conjecture and estimation. As detailed herein, however, our *in camera* scrutiny of the FISA record reveals no additional bases for suppression.

or search to determine whether intelligence-gathering was "lawfully authorized and conducted." Id. The court may disclose "portions of" the underlying applications and supporting materials to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality" of the surveillance or search. Id. Courts interpreting this language have uniformly held that *in camera* and *ex parte* hearings are the "rule" and that disclosure is the "exception, occurring *only* when necessary." Duggan, 743 F.2d at 78; United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982).

The government correctly observes that every court but one to have addressed a similar motion has found disclosure to be unnecessary. (Doc. 71 at 23-25 (collecting cases)). The only district court to order disclosure was overturned swiftly on appeal. See United States v. Daoud, No. 12-CR-723, 2014 WL 321384, at *3 (N.D. Ill.), rev'd, 755 F.3d 479, 481-85 (7th Cir.), reh'g *en banc* denied, 761 F.3d 678 (7th Cir. 2014), cert. denied, 135 S. Ct. 1456 (2015). But to the extent the government intimates that disclosure is inappropriate merely because it is unprecedented, we reject the suggestion. That disclosure has not previously been ordered does not foreclose the possibility.

Moreover, the court questions whether this consensus accurately reflects Congressional intent. The statute is explicit in acknowledging that there may arise circumstances when "disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f), 1825(g). The legislative history reveals that Congress may not have intended to place the disclosure option so far out of reach:

> Thus, in *some* cases, the Court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information. . . . In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part, since such disclosure "is necessary to make an accurate determination of the legality of the surveillance."

S. Rep. No. 95-604, pt. 2, at 58 (1978) (emphasis added) (citing Taglianetti v. United States, 394 U.S. 316, 317 (1969); Alderman v. United States, 394 U.S. 165, 182 n.14 (1968)). We review Aziz's disclosure request scrupulously, adhering to constitutional principles and statutory dictates.

Attorney General Loretta E. Lynch executed a declaration and claim of privilege asserting that disclosure of the FISA materials would harm national security. (Doc. 71-1 ¶ 3). The Attorney General's declaration is supported by classified declaration of Carl Ghattas, Assistant Director of the Counterterrorism Division of the Federal Bureau of Investigation. (See id. ¶ 4). The declarations and assertion of privilege are subject to "minimal scrutiny," and we may not "second-guess" the Attorney General's representations. *In re* Grand Jury Proceedings of Special April 2002 Grand Jury, 347 F.3d 197, 205 (7th Cir. 2003) (citing Duggan, 743 F.2d at 77). In light of this claim of privilege, FISA permits disclosure only if an *in camera* and *ex parte* review of the materials reveals that disclosure is necessary for an accurate determination of the legality of the surveillance or search. 50 U.S.C. §§ 1806(f), 1825(g).

Aziz maintains that the government's failure to disclose FISA materials transgresses the Fourth, Fifth, and Sixth Amendments and eviscerates the very purpose of our adversary system of justice. (Doc. 63 at 43-47, 56-61). Aziz alleges that FISA allows the government to reverse engineer prosecutions, concealing their "most intrusive and controversial surveillance methods . . . in order to thwart any adversarial challenge." (Id. at 53-56). Aziz exhorts that these considerations, both separately and together, jeopardize his right to a fair trial.

Congress was neither unmindful to these concerns nor unaware of its deviation from traditional adversarial practice. In enacting FISA, Congress sought to achieve parity among two critical but competing interests—to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." S. Rep. No. 95-701, at 16 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 3985. The net effect is that a defendant's rights remain protected, not through traditional notice or disclosure channels, but through the "in-depth oversight of FISA surveillance by all three branches of government . . . ." Belfield, 692 F.2d at 148. This system of legislative, executive, and judicial supervision adequately guards a defendant's constitutional rights. Indeed, FISA's *ex parte* review provisions have withstood every Fourth,

Fifth, and Sixth Amendment challenge levied against them.[4] We find no constitutional deficiency in FISA's notice and disclosure provisions.

In providing for *in camera* and *ex parte* review, Congress entrusted district courts to meticulously review the FISA record for any indication of unlawfulness and to authorize disclosure when "necessary" to protect the defendant's rights. 50 U.S.C. §§ 1806(f), 1825(g). This court has complied with the statutory directive. We can fairly characterize the FISA materials in the instant case as "uncomplicated." See, e.g., Belfield, 692 F.2d at 147; United States v. Warsame, 547 F. Supp. 2d 982, 987-88 (D. Minn. 2008); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 310 (D. Conn. 2008). Our inspection reveals no evidence or indication of irregularity, inconsistency, or insufficiency which might warrant disclosure to defense counsel of any portion of the FISA materials. See S. Rep. No. 95-604, pt. 2, at 58. The court is fully satisfied that it is able to make the requisite legal determinations on the basis of its *in camera* and *ex parte* review. Disclosure is unnecessary under §§ 1806(f) and 1825(g).

Nor do other authorities cited by Aziz mandate disclosure. Sections 1806(g) and 1825(h) of FISA provide that a court denying a defense motion for disclosure may permit discovery nonetheless "to the extent that due process requires." 18 U.S.C. §§ 1806(g), 1825(h). The act's legislative history makes clear that Congress

[4] See, e.g., United States v. El-Mezain, 664 F.3d 467, 567 (5th Cir. 2011); United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005); United States v. Isa, 923 F.2d 1300, 1306-07 (8th Cir. 1991); Belfield, 692 F.2d at 148-49; United States v. Nicholson, No. 09-CR-40, 2010 WL 1641167, at *3-4 (D. Or. Apr. 21, 2010); United States v. Mubayyid, 521 F. Supp. 2d 125, 130-31 (D. Mass. 2007); United States v. Nicholson, 955 F. Supp. 588, 592 (E.D. Va. 1997); United States v. Falvey, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982).

sought to displace *traditional* discovery in favor of the FISA disclosure provisions to the extent "constitutionally possible." United States v. Thomson, 752 F. Supp. 75, 82 (W.D.N.Y. 1990) (citing H.R. Rep. 95-1283, pt. 1, at 94 n.50 (1978)); United States v. Spanjol, 720 F. Supp. 55, 59 (E.D. Pa. 1989) (same). The due process exceptions of §§ 1806(g) and 1825(h) limit permissible discovery to that which is constitutionally mandated, such as the obligations articulated in Brady v. Maryland, 373 U.S. 83 (1963). Thomson, 752 F. Supp. at 82-83 (quoting Spanjol, 720 F. Supp. at 59). The court's review of the FISA record reveals no exculpatory material that must be disclosed on the basis of Brady and its progeny.

For the same reason, Aziz's invocation of the Federal Rules of Criminal Procedure also falls flat. Aziz suggests that Rules 12 and 16 at minimum demand notice of the methods of surveillance or searches conducted. Congress intentionally replaced these discovery rules with FISA's disclosure framework. See Thomson, 752 F. Supp. at 82; Spanjol, 720 F. Supp. at 59. In other words, Congress "rendered Rule 16 and other existing laws inapplicable to discovery" in the FISA context. Thomson, 725 F. Supp. at 82 (quoting H.R. Rep. 95-1283, pt. 1, at 94 n.50). Federal Rules 12 and 16 do not, and cannot, supersede FISA's statutory prohibition on disclosure.

Aziz's reliance on 18 U.S.C. § 3504 is misplaced. Section 3504 requires the government, in a traditional criminal prosecution, to affirm or deny the occurrence of surveillance when the defendant claims that evidence deriving therefrom is the primary product of an unlawful act. 18 U.S.C. § 3504. Section 3504 concerns only *unlawful* surveillance; it does not require affirmance or denial of *all* surveillance.

Id. § 3504. Further, in cases involving FISA information, a suppression motion pursuant to §§ 1806(e) or 1825(f) "is the procedure clearly contemplated by the foreign intelligence statutes for resolving allegations of unlawful surveillance." United States v. Thomas, No. 15-171, 2016 WL 4409101, at *4, __ F. Supp. 3d __ (E.D. Pa. 2016). FISA's particularized notice, disclosure, and suppression procedures supplant the requirements of § 3504.

Aziz lastly cites to 50 U.S.C. § 1881e for the proposition that FISA "expressly requires" the government to provide him "with notice of some types of surveillance at issue." (Doc. 63 at 49-50). Section 1881e governs the use of information obtained through surveillance conducted under the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 95-511, 122 Stat. 2437 (July 10, 2008), which authorizes surveillance of persons outside of the United States under a reduced government burden. See 50 U.S.C. §§ 1881a-1881g. The cited section merely incorporates FISA's preexisting notice and disclosure provisions, making them equally applicable to the FAA. See id. § 1881e. Section 1881e does not establish additional notice and disclosure requirements.

A defendant's constitutional rights necessarily exist in counterpoise with all citizens' collective interest in our nation's security. *In camera* and *ex parte* review adequately preserves both interests. The court will deny Aziz's motion for notice and disclosure of the government's applications.[5]

[5] Defense counsel's offer to obtain requisite security clearances neither abates nor overrides FISA's concerns. See Daoud, 755 F.3d at 484-85; El-Mezain, 664 F.3d at 568. Counsel's possession of requisite clearance is immaterial until and unless a defendant demonstrates that disclosure of FISA materials is "necessary."

B. Request for Franks Hearing

Aziz also requests that the court convene a Franks hearing to allow counsel to test the veracity of the FISA applications. A criminal defendant may challenge the truthfulness of factual statements in an affidavit of probable cause through what is commonly referred to as a Franks proceeding. See Franks v. Delaware, 438 U.S. 154 (1978). When a defendant makes "a substantial preliminary showing" that the affidavit in question contains a false statement which was both knowingly or recklessly made and material to the finding of probable cause, the court must conduct an evidentiary hearing to examine the sufficiency of the affidavit. United States v. Yusuf, 461 F.3d 374, 383 (3d Cir. 2006) (citing Franks, 438 U.S. at 171). Knowing or reckless omissions will also trigger a Franks hearing if the affidavit, including the omitted fact, would not establish probable cause. Id. at 383-84.

At minimum, the defendant's preliminary showing must include an "offer of proof." United States v. Chandia, 514 F.3d 365, 373 (3d Cir. 2008). Sufficient proof includes "affidavits or sworn or otherwise reliable" statements. Id. Courts within the Third Circuit and elsewhere have assumed, without deciding, that Franks' underlying principles apply in the FISA context. See United States v. Shnewer, No. 07-459, 2008 U.S. Dist. LEXIS 112001, at *35-38 (D.N.J. Aug. 14, 2008) (citing Damrah, 412 F.3d at 624-25; Duggan, 743 F.2d at 77 n.6; Mubayyid, 521 F. Supp. 2d at 130).

Aziz's efforts to meet his preliminary burden are necessarily speculative. The court is not insensitive to the plight of defense counsel, who must endeavor to establish the falsity of statements that the law does not allow him to see. On the

other hand, the court cannot repudiate FISA's disclosure provisions by granting full access to classified material when a defendant lodges conjectural allegations of impropriety. In the exceptional context of FISA cases, the defendant's preliminary burden for a Franks review is all but insurmountable. See Shnewer, 2008 U.S. Dist. LEXIS 112001, at *37-38 (describing burden as "seemingly impossible"); Mubayyid, 521 F. Supp. 2d at 131 (acknowledging "the difficulty of defendants' position"). In recognition thereof, Congress mandated careful *ex parte* and *in camera* judicial review of the FISA record. In essence, the court's independent review may supplant that of defense counsel.

Aziz suggests the "possibility" of error in the government's affidavits. (Doc. 63 at 37). He cites to the FISC's 2002 decision in *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. 2002), which acknowledged an uptick of reported misstatements in FISA applications between March 2000 and mid-2001. Id. at 620-21. We reject this argument. There is no indication that these errors have persisted. To the contrary, the FISC noted that the Federal Bureau of Investigation thereafter "promulgated detailed procedures governing the submission of requests to conduct FISA surveillance and searches" in an effort to remedy the problem. Id. at 621. In any event, the FISC's remarks do not increase the likelihood of a misstatement here. As one court observed: the FISC's appraisal of generalized errors is no more probative of an error in this case "than a general study of errors committed over a period of years in baseball would be probative of whether errors occurred in a specific game." United States v. Rosen, 447 F. Supp. 2d 538, 552 (E.D. Va. 2006).

Aziz also cites a 2006 Department of Justice report which found that FISA-related "over-collections" and "overruns" comprised sixty-nine percent (69%) of reported intelligence violations in 2005. (Doc. 63 at 38-39). "Over-collection" refers to information gathered within the period authorized by an FISC order but beyond the order's substantive scope. See U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, REPORT TO CONGRESS ON IMPLEMENTATION OF SECTION 1001 OF THE USA PATRIOT ACT 24 (2006). "Overrun" refers to FISA activity conducted beyond the temporal scope of an order. Id. at 24-25. Without minimizing the significance of these findings, we note that they raise doubts only as to agency compliance with orders once received—they contain no express or implied observations regarding the accuracy of FISA applications themselves. See id. at 29.

As noted, the court has reviewed the entire FISA record. We have found no evidence or indication of a material misstatement or omission therein. In sum, there is no arguable basis for the court to convene a Franks hearing.

C. The FISA Application

We turn now to Aziz's allegations that the government may have failed to comply with FISA in application for or execution of the surveillance and search orders in this case. Pursuant to §§ 1804(a) and 1823(a), every application must:

> (1) identify the officer making the application;
>
> (2) identify or describe the target and, in the case of a physical search, describe the property or premises to be searched and the information, material, or property to be seized;
>
> (3) state the facts and circumstances supporting the applicant's belief that:

(a) the target of the surveillance or search "is a foreign power or the agent of a foreign power";

(b) the facility to be surveilled or the premises to be searched is or is about to be owned or used by a foreign power or an agent of a foreign power; and

(c) in the case of a physical search, the premises or property to be searched contains foreign intelligence information;

(4) state the proposed minimization procedures;

(5) state the nature of the foreign intelligence information sought and, in the case of surveillance, describe "the type of communications or activities" to be surveilled;

(6) describe, in the case of surveillance, the manner in which the surveillance will be conducted, including whether physical entry is required, and, in the case of physical search, the manner in which the search will be conducted;

(7) include an appropriate certification by a statutorily-designated official, the requirements for which are detailed *infra*; and

(8) state all facts concerning previous FISA applications involving any of the persons, facilities, or places subject to the application, and the disposition of each such application.[6]

50 U.S.C. §§ 1804(a), 1823(a). Applications for electronic surveillance must identify the proposed duration thereof. Id. § 1804(a)(9).

Each application must also include a certification by a designated executive branch official with national security responsibilities that:

(1) the "official deems the information sought to be foreign intelligence information";

[6] The requirements for a FISA application vary slightly depending on the form of intelligence-gathering sought. Compare 50 U.S.C. § 1804(a) (electronic surveillance) with § 1823(a) (physical search). The above description combines the requisite elements of both statutory provisions.

(2) a "significant purpose" of the surveillance or search is to obtain foreign intelligence information;

(3) the information sought "cannot reasonably be obtained by normal investigative techniques";

(4) designates the foreign intelligence information sought according to categories set forth in 50 U.S.C. § 1801(e); and

(5) states the basis for the official's certification that the information sought is the type of intelligence designated and cannot reasonably be obtained by normal techniques.

Id. §§ 1804(a)(6), 1823(a)(6). Foreign intelligence information includes "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power" or "sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power." Id. § 1801(e)(1). It also includes "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to . . . the national defense or the security of the United States . . . [or] the conduct of the foreign affairs of the United States." Id. § 1801(e)(2). The phrase "United States person" means, among others, citizens and lawful permanent residents of the United States. Id. § 1801(i).

The assigned FISC judge may enter an *ex parte* order approving an application made under §§ 1806(a) or 1823(a) only if he or she finds that: (1) the application is filed by an appropriate federal officer and has been approved by the Attorney General; (2) there is probable cause to believe that the identified target is a

foreign power or an agent thereof and, if the target is a United States person, the application is not made "solely upon the basis of activities protected" under the First Amendment; (3) there is probable cause to believe that the facilities or places to be surveilled or searched are in use or about to be used by a foreign power or an agent of a foreign power; (4) the applicant's proposed minimization procedures satisfy the minimization requirements set forth in 50 U.S.C. § 1801(h); and (5) the application contains all requisite statements and certifications. Id. §§ 1805(a), 1824(a). If the target of the surveillance or search is a United States person, the FISC must further find that the certifications are not "clearly erroneous." Id. §§ 1805(a)(4), 1824(a)(4).

1. *Standard of Review*

The parties dispute the appropriate manner of review. Unlike most aspects of FISA interpretation, federal courts disagree with respect to the proper standard for review of FISC probable cause determinations. A minority of courts have held that a standard deferential to the FISC is appropriate.[7] The more robust line of

[7] See Abu-Jihaad, 630 F.3d at 130-31. We note that the Second Circuit's decision in Abu-Jihaad appears to be based on a misreading of a prior opinion, United States v. Duggan, wherein the court observed that FISA *certifications* are reviewed—both by the FISC and district courts—with "minimal scrutiny." Abu-Jihaad, 630 F.3d at 130-31 (quoting Duggan, 743 F.2d at 77). With the exception of district courts within the Second Circuit, only one other district court has adopted the deferential standard. See United States v. Ahmed, No. 06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *21-22 (N.D. Ga. Mar. 19, 2009).

authority concludes that a *de novo* standard applies.[8] The government suggests that a deferential standard is more appropriate, likening our examination of FISA's warrant-like orders to the obeisant review traditionally accorded to a magistrate judge's finding of criminal probable cause. (See Doc. 71 at 32-33).

The court rejects the government's analogy. The *ex parte* nature of FISA proceedings gainsays any such comparison. By virtue of the statute's disclosure provisions, a FISA target cannot examine or meaningfully challenge the sufficiency of the United States' application. The statutory scheme requires the defendant and his counsel to place their trust singularly in the reviewing court. If the Fourth Amendment is to retain meaning under such circumstances, it demands—at minimum—*de novo* review.

Accordingly, the court examines anew all of the government's applications. Certificates appended to the applications are entitled to a "presumption of validity" by statute. Rosen, 447 F. Supp. 2d at 545 (citing 50 U.S.C. § 1805(a)(5)). Otherwise, we accord no deference to the applications themselves, nor to the FISC's probable

[8] See United States v. Hassan, 742 F.3d 104, 138-39 (4th Cir. 2014); United States v. Wright, No. 15-10153, 2016 WL 7469712, at *1, __ F. Supp. 3d __ (D. Mass. 2016); United States v. Huang, 15 F. Supp. 3d 1131, 1138 (D.N.M. 2014); United States v. Sherifi, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); United States v. Alwan, No. 1:11-CR-13, 2012 WL 399154, at *8 (W.D. Ky. Feb. 7, 2012); Kashmiri, 2010 WL 4705159, at *1; Nicholson, 2010 WL 1641167, at *5; United States v. Gowadia, No. 05-486, 2009 WL 1649709, at *4 (D. Haw. June 8, 2009); Warsame, 547 F. Supp. 2d at 990; Mubayyid, 521 F. Supp. 2d at 131; Rosen, 447 F. Supp. 2d at 545; see also United States v. Ali, 799 F.3d 1008, 1022 (8th Cir. 2015) (noting discord and resolving that the record satisfied either standard); United States v. Hussein, No. 13-CR-1514, 2014 WL 1682845, at *4 (S.D. Cal. Apr. 29, 2014) (same); United States v. Hasan, No. 12-MC-195, 2012 WL 12883086, at *4 (W.D. Tex. Aug. 14, 2012) (same).

cause findings. We must determine independently whether the applications are adequately supported by probable cause.

Aziz advances a threefold challenge to the legality of the FISA collection. He asserts: *first*, that the applications do not establish requisite probable cause; *second*, that the applications may not comply with the statute's manifold requirements; and *third*, that the government may have exceeded its authority under the resulting FISC orders.

2. *Significant Purpose*

Aziz first confronts FISA's "significant purpose" requirement. Specifically, he asserts that the reduced standard accomplished by the Patriot Act compromises constitutional rights by circumventing criminal warrant requirements, effectively bypassing the Fourth Amendment under the banner of foreign intelligence gathering. (See Doc. 63 at 11 n.1, 66-68). Aziz acknowledges that this argument has been unanimously rejected by every court to consider it, but implores that a changing intelligence-gathering environment and enhanced public scrutiny dictate a jurisprudential change of course. (See id.)

Our response to this entreaty begins and ends with the Third Circuit's decision in United States v. Duka, 671 F.3d 329 (3d Cir. 2011), which expressly holds that FISA's "significant purpose" test is constitutional. Id. at 343. The court noted that the standard reflects Congress's intent to achieve appropriate accord "between 'the legitimate need of Government for intelligence information' and 'the protected rights of our citizens.'" Id. (quoting United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 323 (1972)). Setting aside any deference to Congressional intent, the court

further held that the standard is independently reasonable, given the irrefutable "high stakes" of national security. Id. at 344. The court emphasized that FISA's "significant procedural safeguards" guard against abuse. Id. at 345. A unanimous consensus of federal decisions support Duka's holding. See Abu-Jihaad, 630 F.3d at 120 (collecting cases).[9]

To the extent Aziz reiterates blanket constitutional challenges to FISA's "significant purpose" amendment, his argument is foreclosed by binding Third Circuit precedent. The court cannot conclude that the balance conceived by Congress and upheld by the Third Circuit (and every other court to address the question) is unreasonable or otherwise violative of the Constitution. For this reason, the court rejects Aziz's facial challenge to FISA, as amended by the Patriot Act. Further, in light of FISA's straightforward application to this case, the court finds no basis for an as-applied challenge.

The court would be remiss if it did not acknowledge Aziz's reference to mounting public distrust of government intelligence-gathering processes, especially in the wake of public disclosure of several controversial programs. One district court recently addressed these issues. The defendant in United States v. Wright, No. 15-10153, 2016 WL 7469712, __ F. Supp. 3d __ (D. Mass. 2016), raised many of the same constitutional and policy concerns articulated by Aziz. Wright cited an increase in controversial intelligence-gathering techniques and attendant public

[9] Only one district court has held that the "significant purpose" standard violates the Constitution, but the Ninth Circuit Court of Appeals overturned the decision. Mayfield v. United States, 504 F. Supp. 2d 1023, 1042-43 (D. Ore. 2007), rev'd on other grounds, 599 F.3d 964, 969-73 (9th Cir. 2010).

unease as a basis for reconsidering the consensus of FISA's constitutionality. Wright, No. 15-10153, Doc. 87 at 29-32 (D. Mass. June 17, 2016).[10]

The district court ultimately rejected each of Wright's arguments, yet expressed its concern over the unyielding shroud of secrecy that cloaks the entire FISA process. See Wright, 2016 WL 7469712, at *1-2. The court cited two factors responsible for the public's escalating skepticism: government over-classification of its intelligence information, and media over-simplification of intelligence-collection processes. Id. The court resolved that it is the task of the judiciary to "patrol the boundaries of the Fourth Amendment" in order to rectify any perceived injury to the public trust. Id. at *2-3.

We have undertaken a thorough "patrol" of the record, and we harbor no doubt about government compliance with the letter of the law. The FISA materials reveal that an appropriate high-ranking government official certified that "a significant purpose" of the surveillance and searches was to obtain foreign intelligence information. These certifications are supported in abundance by the record before the FISC. The court is also confident that obtaining foreign intelligence was the *primary* purpose of the government's efforts. The court concludes that the government's applications satisfy FISA's purpose element.

[10] On the issue of perceived abuses of the intelligence-gathering process, the court notes with interest that the defense brief in Wright and that submitted by defense counsel in the instant case are virtually identical. Compare Wright, No. 15-10153, Doc. 87 at 29-32, with (Doc. 63 at 63-68).

3. *Probable Cause*

The FISA probable cause inquiry differs from the familiar standard applicable to traditional criminal search warrants. The statute concerns not the target's commission of a crime, but instead a target's status as "a foreign power or an agent of a foreign power." 50 U.S.C. §§ 1805(a)(2), 1824(a)(2). The term "foreign power" includes groups "engaged in international terrorism or activities in preparation therefor." Id. § 1801(a)(4). An "agent of a foreign power" is any person who:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. § 1801(b).

A United States citizen cannot be designated an agent of a foreign power "solely upon the basis of activities protected" under the First Amendment. Id. §§ 1805(a)(2)(A), 1824(a)(2)(A). A probable cause finding may "rely *in part* on activities protected by the First Amendment, provided the determination also relies on activities not" thereby protected. Rosen, 447 F. Supp. 2d at 548 (emphasis added).

The defendant does not dispute that ISIL is a group engaged in international terrorism or activities in preparation therefor, thus qualifying as a foreign power under § 1804(a)(4). Aziz instead disputes the United States' ability to show that he is an agent acting for or on behalf of that foreign power. (Doc. 63 at 24-26). He suggests, based on evidence disclosed thus far, that the FISA applications were impermissibly based on protected First Amendment activities. (See id. at 34-35). Aziz also refers to controversial intelligence-gathering techniques—to wit: the warrantless Terrorist Surveillance Program and surveillance conducted pursuant to either § 1881a of the FAA or Executive Order 12,333—in questioning the reliability of the information submitted to the FISC. (Id. at 26-34).

The court has retraced the FISC record bearing each of Aziz's concerns in mind. We have no difficulty concluding that the government satisfied all statutory requisites in this case. In each application, the government established probable cause to believe that the target of the surveillance and searches was an agent of a foreign power, and that the facilities, premises, or places to be searched were being used or were about to be used by the agent of a foreign power. See 50 U.S.C. §§ 1804(a)(3), 1823(a)(3). In this regard, the government's filings were quite

detailed, describing at length the many facts supporting its certification that a "significant purpose" of the surveillance and searches was to obtain foreign intelligence information.

We also find that the applications were grounded in conduct which plainly exceeds the bounds of the First Amendment's protective sphere. Hence, the FISC orders in this case do no violence to the target's First Amendment rights. The record is devoid of any evidence that the government's intelligence-gathering efforts in this case fell within any category deemed questionable by defense counsel. The court finds ample probable cause to support the FISC orders.

4. *Procedural and Technical Compliance*

Aziz also asks the court to audit the government's procedural and technical compliance with FISA. (See Doc. 63 at 40-43). As noted, FISA requires the government to attach to each surveillance or search application a certification that the information sought is foreign intelligence information, that a "significant purpose" of the surveillance or search is to obtain such information, and that the foreign intelligence information could not be reasonably obtained through normal investigative techniques. 50 U.S.C. §§ 1804(a)(6), 1823(a)(6). The certification must also identify the type of foreign intelligence information sought and state the basis for the certifying official's belief concerning each of the requisite certifications. Id. We apply a "clearly erroneous" standard of review to the FISA certifications. Id. §§ 1805(a)(4), 1824(a)(4).

Aziz contends that the government's applications may have omitted the requisite certifications or, alternatively, that the certifications were deficient. He

urges the court to carefully measure each certification against the statutory elements. Having done so, we conclude that the FISA record is free of procedural defect. Every application contains the certifications mandated by §§ 1804(a)(6) and 1823(a)(6), and no information or statement contained therein appears to be "clearly erroneous." Id. §§ 1805(a)(4), 1824(a)(4).

Aziz also suggests that the FISA applications may not have established, or the government may not have implemented, requisite minimization procedures. Every FISA application must contain a statement of the government's "proposed minimization procedures." Id. §§ 1804(a)(4), 1823(a)(4). Minimization procedures "are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information." *In re* Sealed Case, 310 F.3d at 731; see 50 U.S.C. § 1801(h). At the acquisition stage, for example, such procedures ensure that a non-target United States person who communicates with a FISA target on a surveilled email account or cellular telephone (about information unrelated to foreign intelligence) will not have those communications publicly disclosed. Rosen, 447 F. Supp. 2d at 551. At the retention stage, intelligence officials must destroy, where feasible, all acquired information that is no longer necessary to ongoing foreign intelligence interests. See *In re* Sealed Case, 310 F.3d at 731; Rosen, 447 F. Supp. 2d at 551. Respecting dissemination, collected information may be used for "approved purpose[s]," but use "should be restricted to those officials with a need for such information." *In re* Sealed Case, 310 F.3d at 731 (quoting H.R. Rep. 95-1283, pt. 1, at 56). The statute does not require minimization of "evidence of a crime." 50 U.S.C. § 1801(h)(3).

Importantly, minimization requirements "are subject to a rule of reason." Rosen, 447 F. Supp. 2d at 553. Congress did not intend for nominal failure to abide the minimization procedures to undercut entire investigations. See S. Rep. No. 95-701, at 21-22. FISA's legislative history reflects that Congress envisioned "the court's role" as determining "whether a good faith effort to minimize was attempted." Id. at 39-40 (quoting United States v. Armocida, 515 F.2d 29, 44 (3d Cir. 1975)). In this assessment, we consider whether agents have demonstrated "a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion." Id. (citations omitted); see also Medunjanin, 2012 WL 526428, at *12; Rosen, 447 F. Supp. 2d at 553.

Each of the government's applications sets forth minimization procedures in compliance with FISA. The government acknowledges that its agents failed to abide certain minimization procedures with respect to a small portion of its intelligence collection. (Doc. 71 at 52). In its classified filing, the government fully and candidly describes the limited scope of this error and details the steps taken to remedy it upon discovery. The court has scrutinized the applicable materials and concludes that this error is *de minimis* and will not prejudice the defendant at trial or otherwise.

Lastly, the court addresses Aziz's concerns with regard to potential over-collections or overruns beyond the substantive or temporal scope of the resulting FISA orders. The court has reviewed each order's issue date and expiration date, as well as returns of the surveillance and searches conducted under those orders.

There is no lapse between operative orders, nor is there any indication of over-collection or overrun in any instance.

IV. Conclusion

In closing, we assure the defendant and defense counsel that we have exhaustively studied the record in this case. The government has strictly complied with the requirements of FISA in its investigation and prosecution of this case. The court concludes that there is no basis to disclose or to suppress the FISA materials.

For the reasons stated herein, the court will deny Aziz's motion. An appropriate order shall issue.

/S/ CHRISTOPHER C. CONNER
Christopher C. Conner, Chief Judge
United States District Court
Middle District of Pennsylvania

Dated: January 12, 2017